DECOIT

User-Centric Identity Management

in mobilen Szenarien im SIMOIT-Projekt

Prof. Dr.-Ing. Kai-Oliver Detken
URL: http://www.decoit.de
URL2: http://www.detken.net
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

Inhalt

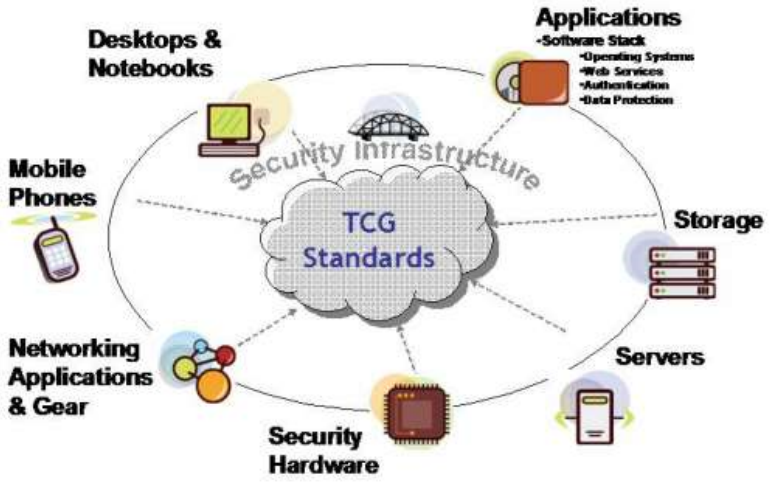
- Problematik
- IT-Sicherheitsfaktoren
- Lösungen für Endpunkt-Sicherheit
- User-Centric Identity Management mit TNC
- Der SIMOIT-Ansatz
- Fazit und Ausblick

Problematik (1)

- Identity und Access Management (IAM) gewinnt zunehmend an Bedeutung für zukünftige Netze und Dienste – besonders für mobile Szenarien
- Durch die Vielfalt der Netzzugangstechnologien sowie durch die steigende Zahl der Dienste, sind mobile Endgeräte zusätzlichen Sicherheitsrisiken ausgesetzt
- Verlässliche Identifikation (Benutzer und Endgerät) zur Autorisierung und Authentifizierung bei Zugängen zu Netzen und Diensten, ist daher zwingend erforderlich
- Der Ansatz Trusted Network Connect (TNC) ermöglicht standardkonform diese Umsetzung

Problematik (2)

- Die TNC-Kernspezifikation wurde bereits abgeschlossen und einige Produkte sind bereits verfügbar
- Eine nahtlose Integration von mobilen Benutzern durch ein „User-Centric Identity Management" ist aber noch nicht möglich
- Authentifizierungsmechanismen und Synchronisation von Benutzeridentitäten sowie -rechten sind bisher nicht kompatibel



IT-Sicherheitsfaktoren

- Ganzheitliche Sicherheit in einer IT-Infrastruktur verlässt sich im Wesentlichen auf folgende Faktoren
  - Zugangssteuerung/Zugriffskontrolle
  - Integrität
  - Originalität (Authentizität)
  - Authentifizierung
  - Autorisierung
  - Vertraulichkeit
  - Verfügbarkeit
  - Audit

Lösungen für Endpunkt-Sicherheit

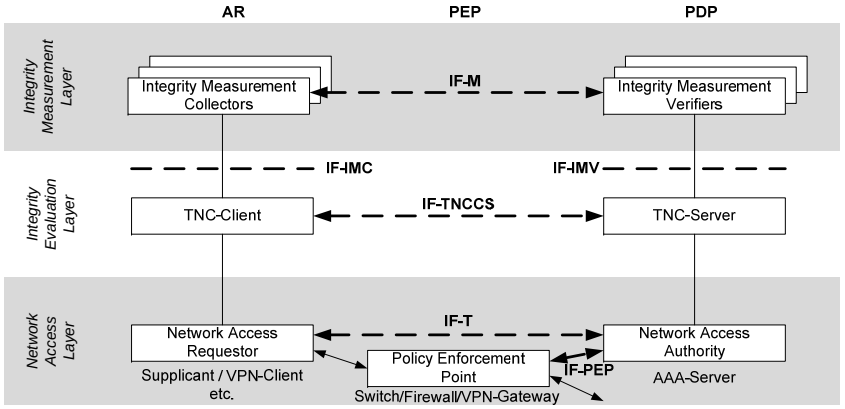
- Endpunkt-Sicherheitslösungen nutzen Router, Switches, WLAN-Access-Points, Software und Security-Appliances
- Es werden Authentifizierungs- und Autorisierungsinformationen über mobile Endgeräte an einen Policy-Server weitergeleitet, der dann entscheidet, ob das Gerät einen Zugang erhalten darf oder nicht
- Der Zugriffsschutz ermöglicht weiterhin, eine Zustandsprüfung („Health Check“) am Client durchzuführen
- Neben den lizenzpflichtigen Softwarelösungen Ciscos Network Admission Control (NAC) und Microsofts Network Access Protection (NAP), gibt es Open-Source-Lösungen, wie den Ansatz Trusted Network Connect (TNC)

Der TNC-Ansatz

- Mit der Trusted Network Connect-Spezifikation (TNC) entwickelt die Trusted Computing Group (TCG) einen eigenen NAC-Ansatz
- Die Entwicklung findet durch die Trusted Network Connect-Subgroup mit über 75 vertretenen Firmen statt und liegt aktuell (April 2008) in der Version 1.3 vor
- Ziel ist die Entwicklung einer offenen, herstellerunabhängigen Spezifikation zur Überprüfung der Endpunkt-Integrität
- TNC baut auf vorhandene Technologien auf, wodurch eine einfachere Integration in bestehende Infrastrukturen möglich ist
  - Netzwerkzugriff: 802.1x, VPN, PPP
  - Nachrichtentransport: EAP, TLS & HTTPS
  - Authentifizierung: Radius Server, Diameter

Überprüfung der Vertrauenswürdigkeit

- Richtlinien-abhängige Zugriffssteuerung für Netzwerke
- Integritätsprüfung: Messen des Systemzustands (Konfiguration der Endgeräte) und Überprüfung dieser Zustände gemäß Richtlinien (Assessment-Phase)
- Isolation von potentiell gefährlichen Rechnersystemen bei Nichterfüllung der Richtlinien (Isolation-Phase)
- Wiedereingliederung nach Wiederherstellung der Integrität (Remediation-Phase)
- Erweiterter Integritätscheck möglich (z.B. Binden von Zugangsdaten an ein bestimmtes Rechnersystem, Signierung von Messwerten)

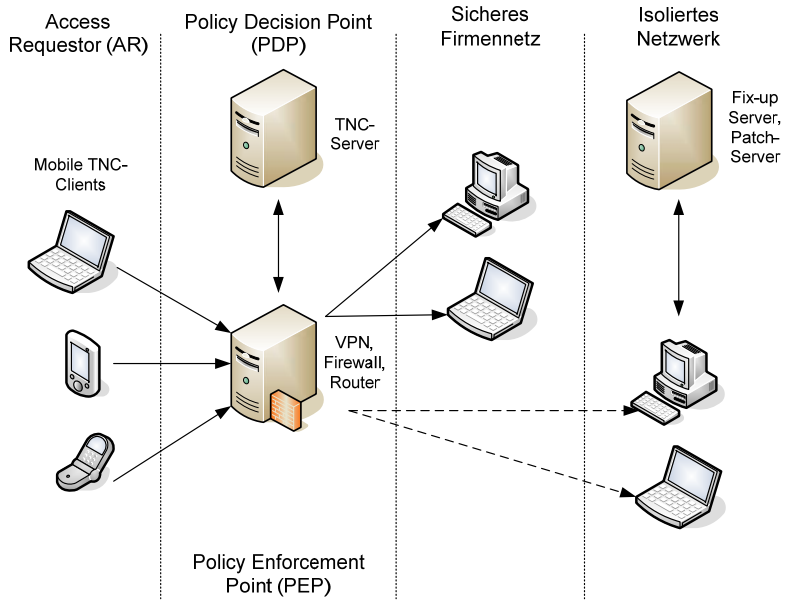


User-Centric Identity Management mit TNC (1)

- Identity Management beinhaltet das Spektrum der Tools, die benutzt werden, um digitale Identitäten zu repräsentieren, administrieren und deren Zugangskontrolle durchzusetzen
- Access Management repräsentiert die zentralisierte Authentifizierung und Autorisierung für die bereitgestellten Netzwerkressourcen
- Hauptziel von Identity- und Accessmanagement (IAM) ist die Verbesserung des angebotenen Dienstes und somit ein einheitlicher Zugriff auf Ressourcen

User-Centric Identity Management mit TNC (2)

- **Access Requestor (AR):** Das Client-System wird um den TNC-Client erweitert. Dieser ermittelt den aktuellen Zustand des Systems und schickt diesen an den TNC-Server (Network Policy Server). Die Messung der einzelnen Komponenten des Rechnersystems findet durch sog. Integrity Measurement Collectors (IMC) statt.
- **Policy Enforcement Point (PEP):** Der PEP ist das TNC-Element am Eintrittspunkt des Netzwerkes; in der Regel eine aktive Netzwerkkomponente (z.B. WLAN Access-Point) mit 802.1x-Unterstützung. Aufgaben der Komponente ist die Entgegennahme und Weiterleitung von Verbindungsanfragen sowie die Ausführung der Handlungsentscheidung des PDP.
- **Policy Decision Point (PDP):** Dieser ist für die Bewertung der durch die Integrity Measurement Collectors ermittelten und durch den TNC-Client übertragenen Messdaten zuständig. Hierfür wird das System um eine Softwarekomponente, den TNC-Server, erweitert, der die Daten vom Client entgegen nimmt. Die eigentliche Bewertung erfolgt durch die Integrity Measurement Verifiers (IMV).



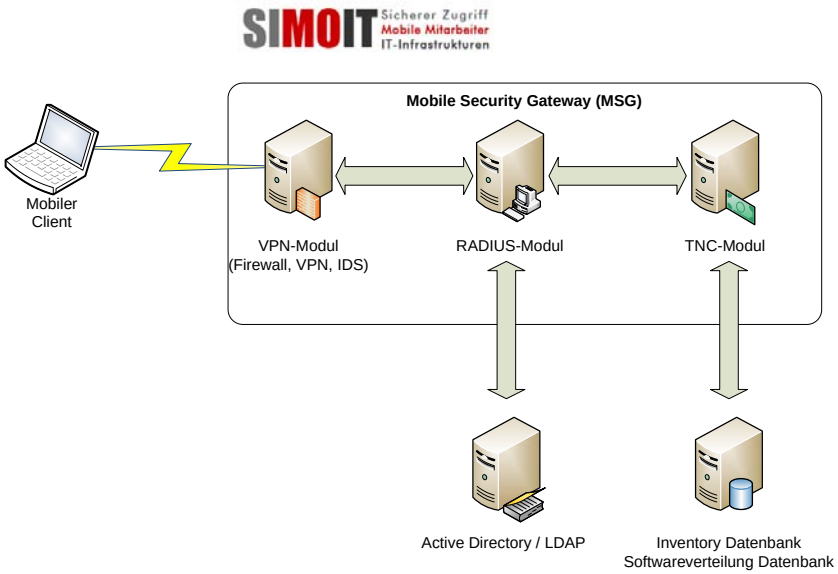
Zielsetzung des Projekts

SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

- SIMOIT = SIcherer Zugriff von MObilen Mitarbeitern auf die IT-Infrastruktur von mittelständisch geprägten Unternehmen
  - Das SIMOIT-Projekt zielte auf die Entwicklung einer auf Standards basierten mobilen IT-Sicherheitsplattform ab, die sich in heterogenen mobilen Umgebungen einsetzen lässt
  - Die in diesem Projekt erarbeiteten Lösungen sollen in unterschiedlichsten Unternehmen einsetzbar sein
  - Ziel war es, technische und auch nicht technische Lösungen als Baukastensystem zu entwickeln, die herstellerunabhängig entwickelt werden
  - Die nicht technischen Lösungen zielen darauf ab die Unternehmensführung über die Notwendigkeit der mobilen IT-Sicherheit zu überzeugen und die Akzeptanz der Mitarbeiter bzw. Benutzer zu erlangen

Technische Plattform (1)

- **VPN-Gateway:** dient als Endpunkt des IPsec und nutzt X.509-Zertifikate für die Endgeräte. Durch den IPsec-Tunnel wird mittels L2TP mit PPP die Authentifizierung durchgeführt. Auch die Zertifikats-ID des VPN-Tunnels wird ermittelt und mit den Anmeldedaten an den RADIUS-Server weitergeleitet.
- **RADIUS-Server:** übernimmt die Autorisierung und Authentifizierung des Benutzers und des Gerätes. Er entscheidet aufgrund der Antwort des TNC-Moduls, ob der eingewählte Client Vollzugriff erhält oder lediglich in das Quarantänenetz gelangt.
- **Windows 2003 Active Directory Server:** Im Active Directory liegen die Benutzerdaten, die vom RADIUS-Server abgefragt werden. Es kann auch ein LDAP-Server verwendet werden.
- **Softwareverteilung:** hält die Informationen der installierten bzw. nicht installierten Paketen vor. Diese Informationen werden vom RADIUS-TNC-Modul ausgewertet.



Technische Plattform (2)

- VPN
  - OpenSWAN
  - xl2tpd
  - pppd
  - radiusclient
- Firewall
  - iptables
- IDS
  - Snort
  - ACIDBASE

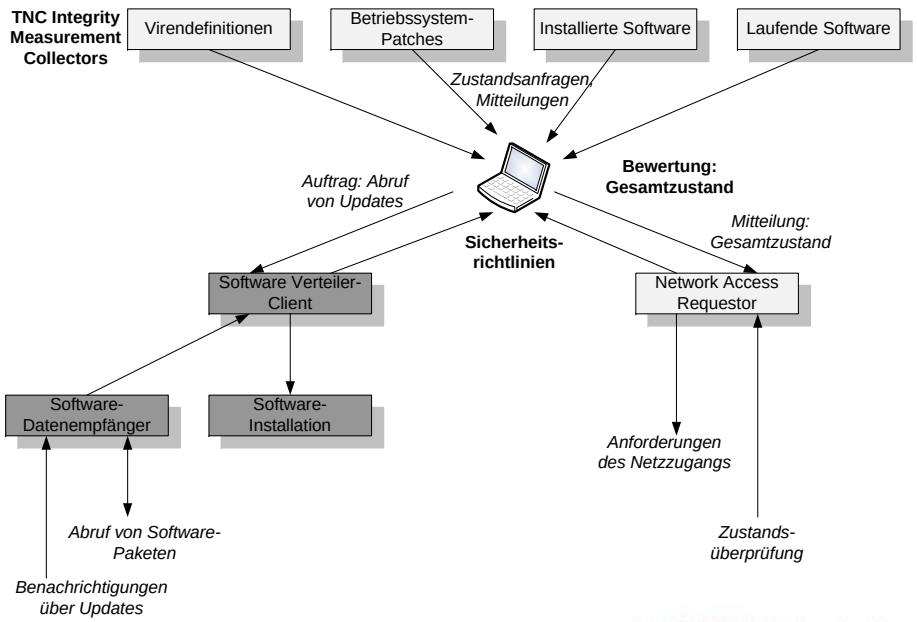
- freeRADIUS
  - LDAP-Autorisierung
  - Authentisierung (Samba / Winbind): User und Passwort werden gegen AD geprüft
- freeRADIUS-Module
  - LDAP
  - MS-CHAP
  - TNC-Server (libtnc)

Mechanismen der SIMOIT-Quarantänezone (1)

- **Integrity Measurement Collectors:** Erfassen den aktuellen Zustand des Systems für definierte Teilbereiche, wie z.B. den Stand der Virendefinitionen oder die Version von Sicherheitssoftware.
- **TNC-Client:** Sammelt auf Anfrage die Informationen der Kollektoren, um diese für Integritätsentscheidungen des TNC-Servers weiterzuleiten.
- **Network Access Requestor:** Verbindet den Client über das VPN mit dem Unternehmensnetz. Bietet in der Authentisierungsphase den Kanal für die Übertragung von Zustandsinformationen zum TNC-Server und Sicherheitsrichtlinien zum TNC-Client.
- **Softwareverteiler-Client:** Falls der Client die Softwarebestandsanforderungen nicht erfüllt, lässt der TNC-Client anhand der Security Policy die jeweilige Komponente neue Softwarepakete installieren.
- **Software-/Datenempfänger:** Empfängt Benachrichtigungen über neue Softwareversionen und aktualisierte Security Policys, um automatisiert den Softwarebestand auf dem aktuellen Stand zu halten. Außerdem ruft diese Komponente nach Anweisung durch den Softwareverteiler-Client die Softwarepakete ab und stellt sie der Softwareinstallation zur Verfügung.
- **Softwareinstallation:** Nach dem Abruf von Installationspaketen sorgen automatisierte Installationsabläufe für eine möglichst geringe Belastung des Endanwenders.

Mechanismen der SIMOIT-Quarantänezone (2)

- Zur Überprüfung des Client-Zustandes werden entsprechend der Sicherheitsrichtlinie Software-Versionsstände, zusätzlich installierte Software, laufende Sicherheitsapplikationen und deren Zustand (z.B. Aktualität von Virendefinitionen) analysiert
- Der TNC Integrity Measurement Collector (IMC) liefert dabei jeweils komponentenspezifische Zustandsinformationen, die vom mobilen Sicherheits-Client zusammengetragen werden
- Dadurch kann sichergestellt werden, dass diese Zustandsüberprüfung zu einem identischen Ergebnis kommt wie die Überprüfung des Autorisierungs-Servers
- Auf Serverseite werden die Zustände der Clients während der Authentisierung überprüft
- Wenn diese nicht ausreichen, werden entsprechende Softwarepakete zur Verfügung gestellt, die zum Erreichen des benötigten Zustandes führen



SIMOIT Sicherer Zugriff Mobile Mitarbeiter IT-Infrastrukturen

Erreichte Ziele von SIMOIT

- Sichere Authentifizierung des Benutzers und der vorhandenen mobilen Hardware
- Quarantäneschutzbereich für nicht konforme Endgeräte zum Aktualisieren der Software
- Serverseitige Entwicklung, wodurch mobile Endgeräte unterschiedlicher Art eingebunden werden können
- Modulare Entwicklung (VPN, Firewall, IDS, RADIUS/802.1x, TNC, LDAP, VoIP), wodurch auch andere Hersteller einbezogen werden können
- Unterstützung diverser Standards und Schnittstellen
- Auswahl unterschiedlicher Sicherheitsprofile
- Netzüberwachungswerkzeuge überwachen kontinuierlich den Netzverkehr

Ausblick und Fazit

- Der TNC-Ansatz wird immer noch spezifiziert, liegt aber seit 2008 auch endlich in der Version 1.3 vor
- Hersteller wie Cisco und Microsoft gingen zuerst eigene Wege (Microsoft hat sich inzwischen wieder zum TNC-Ansatz bekannt)
- Andere Hersteller unterstützen ebenfalls den gemeinsamen Standards, so dass von einer erhöhten Kompatibilität und schnelleren Entwicklung ausgegangen werden kann
- SIMOIT hat bisher noch keinen TNC-Client umgesetzt; das Fehlen muss durch die Softwareverteilung kompensiert werden
- Durch zentrale Erfassung der Benutzer und Softwarestände mit Verzeichnisdienstunterstützung wird ein einheitliches Identity Management ermöglicht
- Sicherheitsrichtlinien des Unternehmens können so auf mobile Endgeräte mit verteilt werden

Danke für Ihre Aufmerksamkeit

SIMOIT URL:
http://www.simoit.de

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09

Consultancy & Internet Technologies